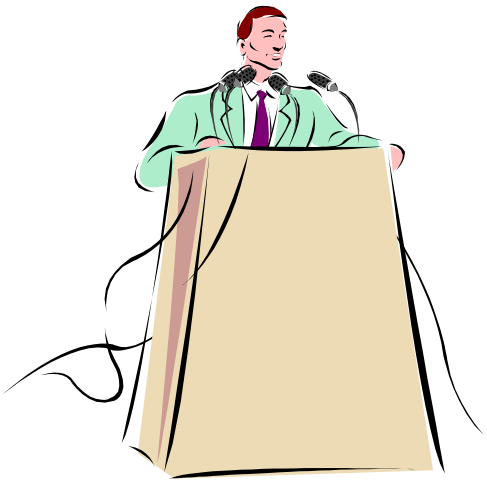
HIPAA
PRIVACY

TRAINING PROCESS

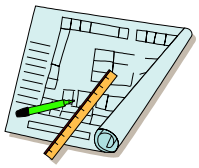


The tools and templates provided in CalOHI Policy and Information Memoranda have generally been authored by HIPAA workgroups. Users should view the information presented in the context of their own organizations and environments. Legal opinions and/or decision documentation may be needed when interpreting and/or applying this information.

TABLE OF CONTENTS

GENERAL INFORMATION

Document Design



In each section of this document, the discussion is divided into two parts: federal HIPAA requirements, and State law requirements. However, please note the only State laws discussed are those **general** laws applying to all health care providers and state government agencies. We have **not** researched or provided specific State law requirements for each program or function. You will need to review the specific mandates below in relation to your programs, functions, and/or business practices:

- Federal laws
- Federal Regulations
- State Laws
- State Regulations
- Departmental administrative manuals

You will need to incorporate all of these into your Privacy Policies and Procedures that address the process you use to facilitate access to protected health information by individuals.

You may find the federal regulations on the CalOHI website on the Privacy page at: CalOHI - Privacy [www.ohi.ca.gov]. The State laws can be found at the California Law page at: Find California Code [www.leginfo.ca.gov], or at the CalOHI website on the Legal page at: CalOHI - HIPAA Rules - Legal Issues [www.ohi.ca.gov]

Throughout the process discussion, you will find red boxes containing Decision Points. Some of these decisions are only for covered entities with specific business practices or specific categories of individuals they serve. You should review the decision points to determine which apply to your business practices. You may consider different alternative solutions to each issue and weigh the positive and negative effects of the alternatives based on your business practices and applicable federal and State laws. We have provided a sample decision tool in the Access Process Package (Exhibit 3 of Policy Memorandum 2003-22) that you can find on the CalOHI website. You may use it as a format when making your decisions. You should also consider your liability and financial impact for each alternative. We recommend you discuss the analyses and recommendations with your legal counsel.

We have provided a checklist of these decision points at the end of this discussion. You should evaluate each decision point to see if it applies to your HIPAA status and/or business practices. You can use the checklist to check off those decisions you will need to make. Once you have established your policies related to these decision points, these policies become part of your Privacy Policies and Procedures.

We have provided examples (in blue ink) to assist in understanding the requirements. Hyperlinks (blue or purple ink) are included in the document. When you are using Microsoft Word and are referred to another location in the document, you can click on the hyperlink and it will send you to the section. If you store all the documents in the same folder, the links between documents will work. We have provided hyperlinks (in blue or purple ink) to web pages or other documents in this package. In addition, you can click on one of the subjects listed in the table of contents and it will take you to the section.

ACKNOWLEDGEMENT

This training package has been developed by a sub-workgroup of the HIPAA Privacy Workgroup and represents a collaborative effort of both state and county representatives. A special thanks for their knowledge, skills, time and effort to:

- Bobbie Holm, California Office of HIPAA Implementation
- Susan Fanelli, Department of Health Services
- David Nelson, Yolo County
- Cheryl Esters, Solano County
- Vonnie Behm, Department of Mental Health

ORGANIZATIONS WHICH HIPAA TRAINING REQUIREMENTS APPLY

Covered Entities

The HIPAA privacy rule requires **covered entities** train all members of its workforce on the policies and procedures with respect to protected health information, as necessary and appropriate for members of the workforce to carry out their functions within the covered entity.

However, the HIPAA privacy rule does not require the following organizations to train their workforce on HIPAA privacy requirements:

- The group health plan provides health benefits solely through insurance contracts with health insurance issuers or HMOS, and
- The group health plans that does not create or receive any PHI for summary health information or information about enrollment.

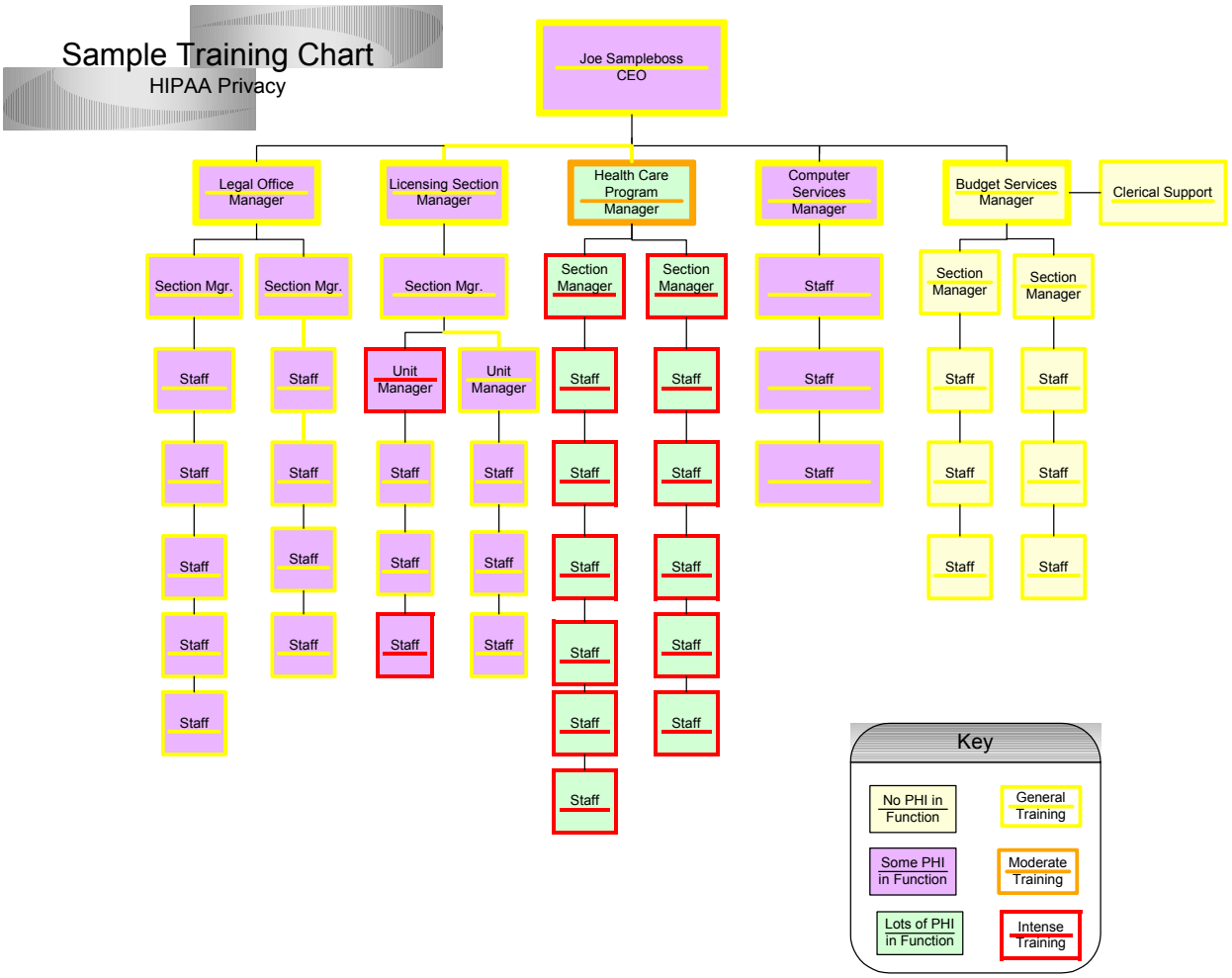
[45 C.F.R. 164.530(k)]

Hybrid Entities

Hybrid entities need to provide training to those portions of their organization they have designated as covered components. They do not need to provide training to the non-covered components if they have established adequate firewalls to prevent the access, use or disclosure of PHI to those members of the workforce in the non-covered components. Many organizations that have declared themselves hybrid entities are choosing to provide general HIPAA training to all members of their workforce regardless of the function within the organization that they perform.

For example, an organization could determine that one function is a covered health care provider and another function is a health plan. In addition, they have a legal office that provides service to the entire organization, a licensing section that licenses providers, a legislative office that provides administrative support to the programs concerning state legislation, a personnel office that provides personnel support, an accounting office that processes billings and payments, and a budget office that provides budget services. Of these, only the health plan and health care provider are covered entities.

But the licensing section, the legal office and the accounting office all need access to some PHI to fulfill their functions. Therefore, three sections must receive training to allow their use of PHI. Other sections such as the Legislative office, personnel office or the budget office would not have access to PHI nor need it to fulfill their functions and would not require training.



Business Associates

Covered entities may require business associates to train their workforce as part of their business associate contract/agreement. Covered entities may choose to provide training to their business associates' work force members to assure compliance with the HIPAA privacy rules.

DECISION POINT: Training for Business Associates – *Will you require or provide privacy training to your business associates?* Covered entities will need to decide if they will require their business associates to either provide HIPAA privacy training to their employees or to provide the training themselves. Some organizations are choosing not to offer covered entities such training to business associates' work forces to avoid any risk of liability that may result.

WHO COVERED ENTITIES MUST TRAIN

All Work Force Members

HIPAA

The HIPAA privacy rule requires covered entities to train all members of their workforce as necessary and appropriate for the members to carry out their functions. This includes all employees, trainees, students, and interns, paid and volunteer, who perform services for your organization. Training of your business associates' work forces is not required.

HIPAA requires that you train your work force to the degree "necessary and appropriate for the member of the workforce to carry out their functions…". Since covered entities are required to train all members of the work force to the degree necessary to carry out their functions, separate levels of training for different workforce groups (e.g., clinical, administrative, support services) may be a more cost-effective approach to training.

DECISION POINT: Impacted Functions – *Have you determined what functions in your organization are impacted by use, disclosure or access?* Covered entities will need to determine which functions in the organization are impacted by the use, disclosure or access to PHI. When the flow of PHI has been mapped, the covered entity finds the location of these functions and identification of workforce members who use, discloses or have access to PHI. Tools for mapping PHI flow were issued with CalOHI Policy Memorandum 2002-13 found at the CalOHI web site: CalOHI - Privacy.

State Law

The Information Practices Act provides that **state departments** must establish rules of conduct and instruct each person about the rules and procedures concerning the privacy of individuals' information. [Civ. Code § 1798.20]

STATE LAW: YOU WILL NEED TO DETERMINE IF YOU SHOULD INCLUDE THE PROVISIONS OF THE INFORMATION PRACTICES ACT (IPA) IN YOUR TRAINING. STATE DEPARTMENTS MAY DETERMINE TO INCLUDE ALL PROVISIONS OF THE IPA IN YOUR TRAINING IF YOU HAVE NOT ALREADY PROVIDED TRAINING ON IT OR IF YOU NEED TO PROVIDE REFRESHER TRAINING.

Which Members/ Which Training

Covered entities will need to look at two factors when determining the level of training to provide to workforce members.

1. The degree of the HIPAA privacy rule's impact on functions
2. The level of functions or activity performed (classifications) within the organization

If the function a workforce member performs entails extensive access, use and/or disclosure of PHI, it increases the risk of a HIPAA privacy violation. Workforce members who perform such functions will need extensive privacy training. Those who have occasional access to PHI may need at least HIPAA privacy overview training, but may also need more moderate training, or specific components of HIPAA privacy training, such as the Access Process and Staffing Requirements.

The members who provide health care to patients will need extensive HIPAA privacy training. Legal counsel, auditors, quality control teams, and licensing staff may need HIPAA privacy overview training and may need some more moderate training depending on the degree of PHI in their function. Members of the licensing staff that license building contractors likely will not need more than overview training while their counterparts who license long term care facilities will need more extensive training.

Level or Classification

A workforce member's level (of classification) may determine the degree of training that they should receive. The levels within an organization may determine the exposure to PHI. Those farther removed from the daily use of PHI will need less HIPAA privacy training than those whose level or classification requires routine use of PHI.

> For example, those in the executive administration of an organization may only need HIPAA privacy overview training, while the members in the training section will need intensive training. Those who are supervisors of members who work with PHI and their staff will need extensive training. Those in middle management, depending on their function may need moderate training.

Covered entities will need to analyze both the function and the level when determining the degree of training to provide to the different members of their workforce.

Combining Both Function and Level

Because of the diversity in most departments and counties, we believe there needs to be at least three types of training:

1. High-level training given to all members of the work force of the covered entity.
2. Moderate-level training for those who manage programs that use or maintain PHI.
3. Detailed training provided in components for those members of the work force whose functions or activities use, disclose, maintain, or have access to PHI.

We recommend high-level general training for the executive staff in the covered entity's organization. We recommend intensive training for the trainers within the organization who will be training the work force and for the immediate supervisors of and the staff members who use, disclose or have access to PHI.

Depending on the function of the member, they may need general HIPAA privacy training, with more extensive training on one or more of the specific components of training.

> For example, the function of staff in the record management section may be retrieval and filing of paper records, with no

---

expectation of any reading of the files. In this situation, stylized training targeted at no further disclosure of file information, no reading beyond what is the minimum necessary, and the penalties for violation of these rules may be adequate. However, if the record management section is the designated contact for access to records by individuals, that function includes retrieving PHI requested by individuals or their personal representatives. Therefore, you will need to expand the training to include the Access Process.

SAMPLE TRAINING DELIVERY BASED ON FUNCTION AND LEVEL

LEVEL	Hospital	Licensing	Eligibility for Services	Health Program Payment Processing	Information Technology	Budgeting	Accounting	Legal Analyses
Executive Staff	General	General	General	General	General	General	General	General
Middle Management	Moderate	General	General	Moderate	General	General	General	General
Direct Supervisors	**Intensive**	General	General	**Intensive**	General	General	General	General
Professional Staff	**Intensive**	Moderate	Moderate	**Intensive**	General	General	General	General
Support Staff	**Intensive**	Moderate	Moderate	**Intensive**	General	General	General	General
Interns/Trainees	**Intensive**	Moderate	Moderate	**Intensive**	General	General	General	General

Decision Point: **Level of Detail in Training** – *What levels of training will you provide?* Covered entities will need to determine which staff to train and the level of detail to provide in the training. You may wish to provide three different levels of detail in the training:

- High-level training for the entire work force
- Medium-level training for those who have minimum use, disclosure or access to PHI
- Intensive training for those who use, disclose or have access to PHI routinely and their supervisors.

This will require designing three different training packages. The factors to consider are the risk of HIPAA privacy violation versus the volume of training when determining the amounts of training to various work force members.

WHEN COVERED ENTITIES MUST TRAIN THEIR WORKFORCE

Current Work Force

Covered entities must complete training of all members of their current work force no later than **April 14, 2003**.

We recommend that covered entities evaluate the risk of violation of HIPAA privacy rule by their workforce members to determine whom to train and in what order. We generally recommend training be provided in the following order:

1. General HIPAA privacy training to all staff
2. Specific intensive training to those members at the greatest risk of violating the HIPAA privacy rule, that is, those who use PHI on a routine basis in their functions
3. Specific training to those who use PHI occasionally in their function or who manage programs where PHI is utilized.

DECISION POINT: Priority of Training – *How will you provide training to new employees?* Covered entities need to determine in what order which functions and levels of staff will be trained.

New Work Force Members

Covered entities must train new staff within a reasonable time.

DECISION POINT: Reasonable Time – New Employees. *When will you provide training to new employees?* Covered entities must determine what a "reasonable time" is. This may be within a set number of days such as 30 days after the start date for the individual. This interval is to be specified in your Privacy Policies and Procedures.

For example, you may decide a person who works daily with PHI must be trained on the HIPAA privacy rule within the first 30 days of working. However, for the other members of your workforce who do not have access to PHI, you may require they receive the high-level training within 120 days of starting work.

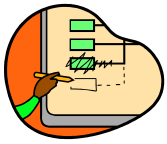
Changes to Privacy Policies and Procedures

Covered entities must train their workforce on changes to their HIPAA Privacy Policies and Procedures within a "reasonable time".

DECISION POINT: Reasonable Time – Changes. *When will you train on changes to your Privacy Policies and Procedures?* Covered entities also need to determine what a "reasonable time" is for training their workforce on changes to their HIPAA Privacy Policies and Procedures. Covered entities may want to establish a consistent definition of "reasonable" times by using the same time limits for:

- New work force members, and
- Changes to policies and procedures

Changes and Renewal



The HIPAA privacy rule requires covered entities to train their workforce initially and when changes occur in the Privacy Policies and Procedures. This would include when DHHS makes changes to the Privacy regulations and when covered entities make changes to their Privacy Policies and Procedures.

DECISION POINT: Training on Changes – *How will you train on changes to the Privacy rule, as well as changes to your Privacy Policies and Procedures?* Covered entities must to determine how they will provide training on changes. If the change to the federal regulations or to the Privacy Policies and Procedures is minor, a simple e-mail to affected work force members may be sufficient. If it is a major change, it may require more formal training.

The HIPAA privacy rule does not require covered entities to renew training to their workforce. However, you may want to consider having a policy on renewal of training. Annual, biennial or triennial training may be desired. Covered entities may consider incorporating the HIPAA privacy training into other training that is required on a regular basis.

DECISION POINT: Renewal of Training – *Will you require on-going retraining?* Covered entities may determine if they will require all or part of their staff to receive retraining on HIPAA privacy.

WHO MAY PROVIDE TRAINING

Contractors, In-House Trainers, Supervisors

Some covered entities contract with consulting firms to provide HIPAA privacy training to their work force. Others may have consulting firms train internal trainers within their organization who will later train their work force.

For example, because of the nature of the HIPAA privacy regulations and their effect on your functions, you may decide to use a combination of these methods.

What basic training and specific Privacy Policies and Procedures training will not provide is exactly how the HIPAA privacy rule will change the business practices of workforce members who do their day-to-day work. Supervisors will need to be well trained so they will be able to train their staff regarding the changes in the business practices that result from the implementation of the HIPAA privacy rule.

DECISION POINT: Trainers – *Who will provide your training?* Covered entities need to determine who will provide the training to their workforce.

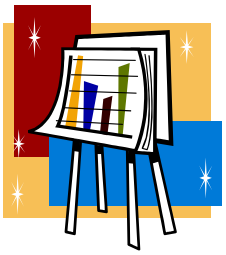
It will be up to the staff and/or their supervisors to bring to the Privacy Officer's attention instances where further policy or procedure changes may need to be made due to:

- Errors in the mapping of PHI flow within the organization
- Errors in the gap analysis of your current business procedures, or
- A HIPAA privacy requirement or function was overlooked in the implementation or updating process, or
- The process is not functioning adequately.

  For example, the current process does not adequately safeguard PHI due to poor storage practices.

WHAT INFORMATION MUST COVERED ENTITIES TRAIN THEIR WORK FORCE ON?

Stylized Training



The HIPAA privacy rule requires that work force members be trained to the extent their functions require it on the covered entity's Privacy Policies and Procedures. In California, this includes:

- The federal HIPAA privacy rule,
- The interaction between the HIPAA privacy rule with the federal laws and regulations that govern the program or function of the covered entity.
- The State laws in conflict with and more stringent than the HIPAA privacy rule, and where HIPAA privacy rule preempts State laws currently in effect
- The covered entities administrative requirements or manuals, and
- The covered entities' policies and procedures [NOTE: Your Privacy Policies and Procedures should include all of the above.]

Some organizations may experience changes in the way they request PHI be disclosed to them. For example, under current practice a law enforcement agency may have access to PHI from a hospital. However, under the HIPAA privacy rule this will change. The law enforcement agency will be limited to the minimum amount of PHI necessary for their purpose. This means that they may need to alter the form and content of their requests. This may occur with other types of organizations, including but not limited to law enforcement, legal representatives, auditing staff, etc. Some organizations are deciding to provide HIPAA privacy rule training about their access limitations to the law enforcement organizations with which they interact to prevent issues arising when law enforcement members no longer have access to information to which they previously had access.

DECISION POINT: Privacy Policies and Procedures – *Do your Privacy Policies and Procedures reflect federal, state and local laws and regulations?* Covered entities must have their Privacy Policies and Procedures completed to include the different federal, state, and/or local laws, regulations and procedures that apply to their program, function or business practices before they will be able to customize their HIPAA privacy training. Customization will enable covered entities to train workforce members on the change in business practices where workforce member's functions or activities are impacted by the HIPAA privacy rule.

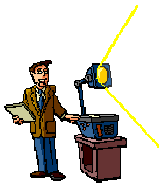
Many organizations have designed a high-level training program with separate individual components to address the parts of the HIPAA privacy rule. For example, separate components of training may be provided for:

- What is Protected Health Information (PHI)
- Complaints
- Access to PHI
- Use of PHI
- Disclosure of PHI
- De-Identification of PHI
- Notices of Privacy Policies
- Privacy Policies and Procedures
- Staffing Requirements – Sanctions,
- Retaliatory Actions, and
- Reporting Violations

Some essential points to include in the training are components on which to train all staff are:

- What is PHI,
- The sanctions and penalties,
- The individuals right to file complaints,
- Workforce members' cannot take retaliatory actions against those who file a complaint, and
- Workforce members' responsibilities to inform the Privacy Officer or other designated person about any breaches in the process or by other work force members; "whistleblower" protection.

Delivery of Training



Training may be provided in a variety of ways:

- Organizations with a large work force with computer access may prefer web-based interactive training. It would provide the advantage of staff convenience to complete the training, automatic scoring, and automatic tracking of completion.
- PowerPoint presentations provided to large groups may be preferable for high-level training that is shorter and less intensive.
- Video training may be used where computer access is not available and the workforce is out-stationed.
- Basic classroom training provided by trainers may be preferred for members of the work force whose functions utilize PHI.

DECISION POINT: Training Delivery – *How will you deliver training?* Covered entities need to decide how they will deliver training to the members of their workforce.

WHAT DOCUMENTATION COVERED ENTITIES MUST MAINTAIN

Documentation

The HIPAA privacy rule requires covered entities to maintain policies and procedures for any action, activity or designation required by the HIPAA privacy rule. Since training is a required activity, the documentation of training must be in a written or electronic record, and include the type of training, when it was conducted, and who received it. This information must be maintained for six years from the date of its creation or the date it was last in effect, whichever is latest. [45 C.F.R. § 164.530(i)]

In addition, the HIPAA privacy rule requires covered entities document what training they provided to the various members of their work force. [45 C.F.R. § 164.530(b)(2)(ii)]

DECISION POINT: Documentation of Training – *What type of training documentation will you maintain?* Covered entities need to determine what type of documentation they will maintain about:

- The training received
- By which members of their workforce
- When

This requirement may be met by different methods including:

- Sign-in sheets at group training classes
- Electronic tracking of individual training through web-based training
- Signed certifications by individuals at the end of training, either classroom or web-based.

Covered entities need to determine if the documentation will be stored electronically or on paper.

The U.S. Department of Health and Human Services (DHHS) requires covered entities to allow access to their records when they are conducting compliance investigations. They may request copies of the training records of the members of the workforce. This may be an easy request to fulfill depending on the location of storage for these records. Covered entities could store records in one of the following ways:

- Each individual supervisor
- Each program
- Each function
- A centralized storage of the records per building
- A central location of these records for the entire organization

A centralized storage would assist in responding efficiently and promptly to a DHHS request or compliance investigation. Other required training programs may have systems in place that could serve as models.

DECISION POINT: Location of Documentation – *Where will you maintain your training documentation?* Covered entities must determine the location(s) of the documentation of training to members of their workforce.

The HIPAA privacy rule does not require some group health plans to document or train their workforce on HIPAA privacy requirements. Such group health plans are those that:

- Provide health benefits solely through insurance contracts with health issuance issuers or HMOS,

and

- Do not create or receive any PHI for summary health information or information about enrollment. [45 C.F.R. § 164.530(k)]

Employee Certification

After providing the training, some organizations are requiring their workforce members to sign a document certifying they understand the HIPAA privacy rule and the organization's Privacy Policies and Procedures. In addition, some organizations are requiring members to sign a document agreeing to meet the HIPAA privacy rule, such as, promising not to divulge any PHI to unauthorized persons or agreeing to report any recognized processes or acts that violate the HIPAA privacy rule. A sample document combining these two requirements is included in this package.

DECISION POINT: Employee Certification – *Will you ask employees to certify their understanding of the Privacy rule?* Covered entities need to determine if they will require employees to certify understanding of the HIPAA privacy rule or to adhere to requirements of the HIPAA privacy rule.

DECISION POINTS

The following table may be used to track the decisions prior to implementing a Training Process.

ISSUE IIMPACTS	DATE STARTED	PERCENT COMPLETED	DATE COMPLETED	ITEM DESCRIPTION
☐				Training for Business Associates
☐				Impacted Functions
☐				Level of Detail in Training
☐				Priority of Training
☐				Intensity of Training
☐				Reasonable Time – New Employees
☐				Reasonable Time - Changes
☐				Training on Changes
☐				Renewal of Training
☐				Trainers
☐				Privacy Policies and Procedures
☐				Training Delivery
☐				Documentation of Training
☐				Location of Documentation
☐				Employee Certification